Our Ref. No. 080398.P245
Express Mail No.: EL236788863US

UNITED STATES PATENT APPLICATION

FOR

COPY-PROTECTING MANAGEMENT USING A USER SCRAMBLING KEY

INVENTOR:
Brant L. Candelore

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Blvd., 7th Floor
Los Angeles, CA 90025-1026
(714) 557-3800

BACKGROUND

1. Field of the Invention

The present invention is related to copy protection. In particular, the present invention is related to copy protection using scrambling keys.

2. Description of Related Art

Copy protection management provides mechanisms to prevent unauthorized copying of clear content. In a typical scenario, a content provider supplies a content to a user via a medium. The medium may be a communication medium such as air, a communication network, or a hardware device, e.g. DVD disk, embodying the content. The content is scrambled by the content provider in a certain way. The scrambled content is then delivered the user's reader or viewing device. The user's reader or viewing device unscrambles the scrambled digital content and provides the content in the clear for viewing, reading, or listening. The clear digital content would typically have copy protection applied to it such as Digital Transmission Copy Protection (DTCP) or watermarking. The copy protection, for example, could limit copying of the clear content to "Copy Never" or "Copy Once".

Conditional access (CA) devices are those user's viewing, reading, or listening devices that provide conditional access to the content. Entitlement management messages (EMM) typically use unique keys or signatures to deliver privileges (e.g., rights, keys) to a particular CA device. Typically, in broadcast systems, a group entitlement right of group key would be delivered to the CA device. Typically the group are users or customers who share a particular set of entitlements, e.g. HBO or Disney.

Current copy protection schemes allow the copying of CA scrambled content as "Copy Free". Yet the CA unscrambled content may or may not be copiable based on the Copy Protection status of the content. A content provider may choose to mark certain types of CA unscrambled content as "Copy Never" where there can never be copying of the CA unscrambled content. In such an approach, the content stored and kept in CA scrambled format. There are a number of problems with such a copy protection approach.

First, if the content is locally scrambled with a unique CA key or unique access right in a particular CA device, then it is difficult to play back the content in another CA device located elsewhere. As an example, in a home environment, if a set-top box has a unique CA key or access right to de-scramble the content delivered by a cable service provider, then only that particular set-top box can provide access to the content. Other set-top boxes located elsewhere (e.g., other rooms, or in the car, or portable devices like a Walkman) cannot access the content.

Second, if the CA device with a unique CA key or unique access right fails to work for any reason, then the content stored with, or received by, that device may not be retrievable. A user's entire archive of movies, music, and other content stored with that unique CA key or unique access right of a particular CA device nay be lost. These and other problems create inconveniences and frustrations for the user, and may also limit the services provided by the content provider.

Therefore, there is a need for a more flexible for handling copy protected content to accommodate multiple access devices.

SUMMARY

The present invention is a method and apparatus for providing copy protection for a content. A descrambler descrambles the content delivered by a content provider using a local key. A key generator is coupled to the descrambler to generate the local key from a programmable user key according to an authorization code provided by the content provider.

In one embodiment, each user is assigned a user key which may be programmed into various devices owned by that user. The user key is used to descramble locally stored content. Scrambled content may be copied since only the devices owned by the user, containing the user key, can unscramble the content. The content may be delivered to the user or household scrambled under the user key. Alternatively, the content may also be delivered under a group entitlement or broadcast key, however when stored locally, the content is reprocessed with the user key.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a diagram illustrating a system in which one embodiment of the invention can be practiced.

Figure 2 is a diagram illustrating a digital receiver according to one embodiment of the invention.

Figure 3 is a diagram illustrating a control processor unit according to one embodiment of the invention.

Figure 4 is a diagram illustrating a conditional access unit according to one embodiment of the invention.

Figure 5 is a flowchart illustrating a process for copy protection for a master CA device according to one embodiment of the invention.

Figure 6 is a flowchart illustrating a process for copy protection for a second CA device according to one embodiment of the invention.

DESCRIPTION

The present invention is a method and apparatus to provide copy protection for a content. The content is provided by a content provider. A descrambler descrambles the scrambled content using a local key. In one embodiment, each user is assigned a user key which may be programmed into various devices owned by that user. The user key is used to descramble locally stored content. Scrambled content may be copied since only the devices owned by the user, containing the user key, can unscramble the content. The content may be delivered to the user or household scrambled under the user key. Alternatively, the content may also be delivered under a group entitlement or broadcast key, however when stored locally, the content is reprocessed with the user key.

A key generator is coupled to the descrambler to generate the local key from a user key according to an authorization code provided by the content provider. In one embodiment of the invention, a communication interface provides the authorization code to the key generator via a communication channel. The technique allows a user to use his or her user key to access a scrambled content with authorized conditional access (CA) devices.

In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well-known architectures, steps, and techniques have not been shown where unnecessary for an understanding of the present invention. For example, specific details are not

provided as to whether the method is implemented in a station as a software routine, hardware circuit, firmware, or a combination thereof.

Embodiments of the invention may be represented as a software product having program code segments to perform the necessary tasks corresponding to the elements of the present invention. The program or code segments can be stored in a processor readable medium or transmitted by a computer data signal embodied in a carrier wave, or a signal modulated by a carrier, over a transmission medium. The processor or machine readable medium may include any medium that can store or transfer information. Examples of the processor readable medium include an electronic circuit, a semiconductor memory device, a ROM, a flash memory, an erasable ROM (EROM), a floppy diskette, a compact disk CD-ROM, an optical disk, a hard disk, a fiber optic medium, a radio frequency (RF) link, etc. The processor or machine readable medium may contain various sets of instructions, code sequences, configuration information, or other data. Those of ordinary skill in the art will appreciate that other instructions and operations necessary to implement the described invention may also be stored on the machine-readable medium. The computer data signal may include any signal that can propagate over a transmission medium such as electronic network channels, optical fibers, air, electromagnetic, RF links, etc. The code segments may be downloaded via computer networks such as the Internet, Intranet, etc.

Figure 1 is a diagram illustrating a system 100 in which one embodiment of the invention can be practiced.

The system 100 includes a program data receiver 110, a transmission medium 120, an audio system 130, a digital video recorder or player 140, a disk recording unit 150, a display 160, a control unit 170, and a network CA unit 180.

The program data receiver 110 includes a digital receiver 112 and a decoder 114. The digital receiver 112 receives digital bitstream or data including program data from one or more service providers. Such service or content providers may include terrestrial broadcasters, cable operators, direct broadcast satellite (DBS) companies, companies providing content for download via the Internet, book publisher, software companies distributing software products, or any similar content and/or service provider. The program data may include system information, entitlement control messages, entitlement management messages, content, and other data. System information may include information on program names, time of broadcast, source, method of retrieving and decoding, copy management commands that provide digital receivers and other devices that control how, when, and what program data may be replayed, retransmitted, copied, and/or recorded. These copy management commands may also be transmitted along with entitlement control messages (ECM), which are generally used by the conditional access unit to regulate access to a particular channel or service. Entitlement management messages (EMM) may be used to deliver privileges to the digital receiver 112 such as rights and de-scrambling keys. As known, a decryption or de-scrambling key is generally a code that is required to restore the scrambled data, and may be a function of the rights granted. Finally, content in the program data may include audio and video data, which may be in s scrambled or encrypted or clear format. The decoder 114 receives the extracted program data from the digital receiver 112. The decoder 114 separates the system information from the content, decodes or decompresses

the content to its original form. In one embodiment, the program data receiver 110 is a television set where the digital receiver 112 is a set-top box integrated therein, and the decoder 114 is a Motion Picture Experts Group (MPEG) decoder.

The transmission medium 120 operates to transmit control information and data including program data between the program data receiver 110 and other components in the system 100. The transmission medium 120 may include air, fiber optics, electronic and magnetic media, computer network connection, telephone connection, and any other communication media.

The audio system 130 is coupled to the transmission medium 130 to provide audio services. The audio system 130 may include speakers, an audio player/recorder such as a compact disk player, or other magneto-optical disc that may be used to play and/or record audio data. The digital video recorder/player 140 is coupled to the transmission medium 120 to provide video services. The digital video recorder/player 140 may be used to record analog or digital video, audio, and other data transmissions. In one embodiment, the digital video recorder/player 140 may be used to replay or record the program data received by the program data receiver 110 and transmitted over the transmission medium 120.

The disk recording unit 150 may also be coupled to the program data receiver 110 and other components via the transmission medium 120. The disk recording unit 150 may be a personal computer system, a stand-alone hard disk recording unit, or other disk recording device capable of recording analog or digital audio, video and data transmissions, including the program data received and transmitted by the program data receiver 110.

The display 160 may include a television display, a monitor display or other devices capable of processing and displaying video signals. In one embodiment, the display 160 is a digital television set. The control unit 170 may also be coupled to the transmission medium 120 to coordinate and control the operation of some or each of the components on the system 100, as well as other devices remotely coupled thereto.

The network conditional access (CA) unit 180 may also be coupled to the transmission medium 120. The network CA unit 180 operates to re-scramble program data with content in clear format such that the system 100 supports the simultaneous transmission of program data in clear and scrambled format. The network CA unit 180 may be a CA device that operates as a second CA device in a system embodiment where the program data receiver 110 operates as a master CA device.

Figure 2 is a diagram illustrating a digital receiver 112 according to one embodiment of the invention. The digital receiver 112 includes a control processing unit 210, a tuner 220, a demodulator 230, a conditional access (CA) unit 240, and a demultiplexer 250.

The control processing unit 210 performs control functions for the tuner 220, the CA unit 240 and the demultiplexer 250. The control processing unit 210 may determine the frequency in which a channel is broadcast or otherwise transmitted. The control processing unit 210 may support a graphical user interface (GUI), such as electronic programming guide (EPG) to allow a user to navigate through various channels and program options to select a desired channel or program for viewing, listening, recording and the like. The control processing unit 210 may contain a copy protection manager that provides copy

protection for multiple CA devices according to one embodiment of the present invention.

The tuner 220 selects a frequency of the signal received by the program data receiver 110 (in Figure 1) under the control of the control processing unit 210. The tuner 220 processes, amplifies, digitizes, and generates a bitstream to the demodulator 230.

The demodulator 230 demodulates the bitstream received from the tuner 220 to provide the program data as originally transmitted. The type of demodulation performed by the demodulator 230 depends on the type of transmission as well as the modulation process used in the transmission process. Examples of the demodulation includes quadrature amplitude modulation (QAM) demodulation, quadrature phase shift key (QPSK) demodulation, and vestigial side band (VSB) demodulation. In addition, the demodulator 230 may perform error correction on the received bitstream.

The conditional access unit 240 may be integral or external to the digital receiver 112. The CA unit 240 provides conditional access to the program data as provided by the demodulator 230. The program data is typically scrambled using an access key. The CA unit 240 may be used in an external or split mode. In the external mode, the CA unit 240 de-scrambles the program data content and decrypts the keys externally; e.g., as is the case with the National Renewable Security System (NRSS) conditional access modules. In a split conditional access unit, the program data content is de-scrambled within the digital receiver 112, while the key decryption is done externally, e.g., via a smart card.

The demultiplexer 250 receives the de-scrambled o r unscrambled content from the CA unit 240. The demultiplexer 250 separates the system information

from the content in the program data, and according to one embodiment, parses the program data for packet identifiers that are associated with the system information, audio information, and video information, and then transmits the system information to the control processing unit 210 and the audio and video information to the decoder 114 (in Figure 1).

Figure 3 is a diagram illustrating a control processor unit 210 according to one embodiment of the invention. The control processor unit 210 includes a processor 305, a host bus 310, a host bridge chipset 320, a system memory 330, a peripheral bus 340, a mass storage device 350, and K peripheral devices 360_1 to 360_K. Although the control processor unit 210 is shown external to the conditional access unit 240 (in Figure 2), it can be implemented as part of the CA unit 240.

The processor 305 represents a central processing unit of any type of architecture, such as complex instruction set computers (CISC), reduced instruction set computers (RISC), very long instruction word (VLIW), explicitly parallel instruction set computing (EPIC), or hybrid architecture. The invention could be implemented in a multi-processor or single processor computer system.

The host bridge chipset 320 includes a number of interface circuits to allow the host processor 305 access to the system memory 330 and the peripheral bus 340. The host bridge chipset 320 may include a memory controller and an I/O controller. The memory controller provides an interface to the system memory 330. The I/O controller provides control of I/O functions.

The system memory 330 represents one or more mechanisms for storing information. For example, the system memory 330 may include non-volatile or volatile memories. Examples of these memories include flash memory, read only

memory (ROM), or random access memory (RAM). The system memory 330 contains a copy protection manager 332, a program 334 and a data 336. Of course, the system memory 330 preferably contains additional software (not shown), which is not necessary to understanding the invention.

The peripheral bus 340 provides bus interface to the mass storage device 350 and peripheral devices 360_1 to 360_K. In one embodiment, the peripheral bus 160 is the peripheral component interconnect (PCI) bus.

The mass storage device 350 include CD ROM, floppy diskettes, and hard drives. The mass storage device 350 stores non-volatile information such as programs or data. The mass storage device 350 provides a mechanism to read machine or processor readable media, including a computer program product comprising a computer usable medium having computer program code embodied therein to provide copy protection management. The peripheral devices 360_1 to 360_K include other peripheral devices or controllers such as network interface device, printer controller, keyboard, mouse, tablet digitizer, etc.

Figure 4 is a diagram illustrating a conditional access unit 240 according to one embodiment of the invention. The CA unit 240 includes a de-scrambler 410, a key generator 420, and a communication interface 430.

The de-scrambler 410 receives the scrambled content, such as the bitstream provided by the demodulator 230 shown in Figure 2, and de-scrambles the scrambled content to the clear format. The de-scrambler 410 performs de-scrambling or de-cryption using a local key provided by the key generator 420.

The key generator 420 receives a user key provided by the user or the content provider and generates the local key to the de-scrambler 410. The key generator 420 may be an interface circuit to interface to a communication channel to receive the user key downloaded from system at the site of the service provider or transferred from another or master CA unit.

According to one embodiment of the invention, the user obtains the user key from the service provider to have access to the scrambled content. The user key is programmable. The user is also granted a right to use the user key in multiple CA devices within his or her control. The granting of this right can be manifested by an authorization code.

The user can copy or re-generate the user key in a number of ways. In one embodiment, the user key is transferred from a master CA device to a second CA device by establishing a connection between the master and the second CA devices. In a second CA device, the key generator 420 has an interface to a connection port via line 422 to receive the user key transferred from a master CA device. In a master CA device, the key generator 420 therefore has an interface to a connection port via line 424 so that the user key can be re-generated for transfer to a second CA device. The transfer of the user key from a master CA device or from a user key transmitter (e.g., directly from the service provider) is permitted only if the receiving unit (e.g., the second CA device) has a proper authorization code. The user therefore can transfer his or her user key to any CA device under his or her control according to the right granted as provided by the authorization code.

The communication interface 430 provides the authorization code to the key generator 420 to allow the generation of the local key. The communication

interface 430 receives the authorization code via a communication channel. The communication channel may be a return path of a cable connection, a telephone connection, or a network. The communication interface 430 may be a modem connection to connect directly to the service provider site. The authorization code may be obtained at the time a contract for service is executed between the user and the service provider, or subsequently when the user contacts the service provider for authorization. Alternatively, the user may register to the service provider as a registered owner of the CA device that has the right to access the scrambled content. Subsequently, the authorization code can be provided to the user if evidence of registered ownership is verified.

In one embodiment, the content may be embodied in a medium. The authorization code may accompany the medium at the time of purchase with a specified grant of right. In another embodiment, the authorization code may be entered directly by the user after contacting the service provider to obtain the authorization code. The user key may also be embedded in the medium embodying the scrambled digital content.

Figure 5 is a flowchart illustrating a process 500 for copy protection for a master CA device according to one embodiment of the invention.

Upon START, the process 500 receives a user key from the content provider (Block 510). The user key may be provided by any means. Then, the process 500 receives an authorization code from the content provider (Block 515). The authorization code grants the user a right to duplicate the user key for use in other CA devices.

Next, the process 500 establishes a connection with a second CA device (Block 520). The connection may be established via any means including

electrical connections with connection ports configured for the transfer. Then, the process 500 transfers the user key and optionally the authorization code to the second CA device (Block 530). In one embodiment, the transfer is permitted when the authorization code matches the authorization code stored in the second CA device. Then the process 500 is terminated.

Figure 6 is a flowchart illustrating a process 600 for copy protection for a second CA device according to one embodiment of the invention.

Upon START, the process 600 receives an authorization code via a communication channel (Block 610). The authorization code may be obtained by the user via any means. The authorization code may be entered by the user as instructed by the content provider at the time a contract between the user and the content provider is executed. Then the process 600 establishes a connection with a master CA device or a user key transmitter (Block 620). The master CA device is a device that originally has a user key unique to the user. The user key transmitter may be any mechanism that can transfer the user key to the second device. Then, the process 600 receives the user key from the master CA device or the user key transmitter (Block 630). In one embodiment, the receipt of the user key is permitted only if the authorization code in the second CA device matches the authorization code in the master CA device or in the user key transmitter.

Next, the process 600 generates a local key from the received user key using the authorization code (Block 640). The local key as generated has the same effect as the original user key. Then, the process 600 de-scrambles the scrambled content using the local key (Block 650). The process 600 is then terminated.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the invention pertains are deemed to lie within the spirit and scope of the invention.